

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	:	Daniel Timmermans
	:	
For	:	PROTECTION AGAINST POWER
	:	ANALYSIS ATTACKS
	:	
Serial No.	:	10/587,727
	:	
Filed	:	July 26, 2006
	:	
Art Unit	:	2431
	:	
Examiner	:	Zia, Syed
	:	
Att. Docket No.	:	NL040060US1
	:	
Confirmation No.	:	1413

APPEAL BRIEF

Mail Stop Appeal Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Customer No.

65913

Sir:

Applicant respectfully submits this revised version of Section V of the Appeal Brief in response to the Notification of Non-Compliant Appeal Brief mailed on August 19, 2010. In compliance with the Notification, this response includes “only the defective section” and lists portions of the Specification “by line and page number.”

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites “an electronic circuit for cryptographic processing, comprising: a first combinatorial logical circuit [Fig. 1: 101] (page 7, lines 1-3), having an input, arranged to perform a first set of logical operations (page 7, lines 8-9) on an input data [Fig. 1: 129] (page 7, lines 8-9) at the input and to produce a corresponding first output data [Fig. 1: 131] (page 7, lines 8-9), the first output data [Fig. 1: 131] (page 7, lines 8-9) having a first functional relation to the input data [Fig. 1: 129] (page 7, lines 8-9) for said input data [Fig. 1: 129] (page 7, lines 8-9) within a given range, and a second combinatorial logical circuit [Fig. 1: 103] (page 7, lines 1-3), having an input, arranged to perform a second set of logical operations (page 7, lines 8-9) on an input data [Fig. 1: 129] (page 7, lines 8-9) at said input and to produce a corresponding second output data [Fig. 1: 131] (page 7, lines 8-9), the second output data [Fig. 1: 131] (page 7, lines 8-9) having a second functional relation to the input data [Fig. 129:] (page 7, lines 8-9), said second functional relation identical to said first functional relation for said input data [Fig. 1: 129] (page 7, lines 8-9) within said given range, wherein the first set of logical operations is different from the second set of logical operations (page 7, lines 8-9), and a selector [Fig. 1: 111] (page 7, lines 1-3) for receiving a given input data and dynamically selecting from among the first combinatorial logical circuit [Fig. 1: 101] (page 7, lines 1-3) for performing the first set of logical operations (page 7, lines 8-9) on the given input data and the second combinatorial logical circuit [Fig. 1: 103] (page 7,

lines 1-3) for performing the second set of logical operations (page 7, lines 8-9) on the given input data [Fig. 1: 129] (page 7, lines 8-9) and producing output data [Fig. 1: 131] (page 7, lines 8-9), and wherein the selecting includes inputting the given input data to the input of the selected one of the first [Fig. 1: 101] (page 7, lines 1-3) and second [Fig. 1: 103] (page 7, lines 1-3) combinatorial logical circuits and outputting a selected first cryptographic processing output [Fig. 1: 131] (page 7, lines 8-9), the selected first cryptographic processing output [Fig. 1: 131] (page 7, lines 8-9) being the output of the selected one of the first [Fig. 1: 101] (page 7, lines 1-3) and second [Fig. 1: 103] (page 7, lines 1-3) combinatorial logical circuits.”

Independent claim 5 recites: “An electronic circuit for cryptographic processing, comprising: a combinatorial logical circuit to perform logical operations on input data and to produce an output data, a storage circuit for storing the output data produced by the combinatorial logical circuit, wherein the storage circuit comprises a first encoding means [Fig. 4: 403] (page 11, lines 1-6) for encoding the output data into a first encoded output data [Fig. 4: 427] (page 12, lines 8-10), a storage element [Fig. 4: 401] (page 12, lines 8-10) for retrievably storing the first encoded output data [Fig. 4: 427] (page 12, lines 8-10), a corresponding first decoding means [Fig. 4: 405] (page 11, lines 1-6), arranged for decoding the first encoded output data [Fig. 4: 427] (page 12, lines 8-10) into said output data [Fig. 4: 431] (page 12, lines 16-18) after retrieving the first encoded output data [Fig. 4: 427] (page 12, lines 8-10) from the storage element [Fig. 4:

401] (page 12, lines 8-10), and wherein the electronic circuit is arranged to dynamically control the activation of the first encoding means [Fig. 4: 403] (page 11, lines 1-6) and the corresponding first decoding means [Fig. 4: 405] (page 11, lines 1-6).”

Independent claim 10 recites: “A method of processing cryptographic data, comprising: using a set of logical operations for processing input data and producing output data, storing the output data in a storage element, wherein the storing comprises: encoding [Fig. 4: 403] (page 11, lines 1-6) the output data into an encoded output data [Fig. 4: 427] (page 12, lines 8-10), storing the encoded output data [Fig. 4: 427] (page 12, lines 8-10) in the storage element [Fig. 4: 401] (page 12, lines 8-10), retrieving the encoded output data [Fig. 4: 427] (page 12, lines 8-10) from the storage element [Fig. 4: 401] (page 12, lines 8-10), decoding [Fig. 4: 405] (page 11, lines 1-6) the encoded output data [Fig. 4: 427] (page 12, lines 8-10) retrieved from the storage element [Fig. 4: 401] (page 12, lines 8-10), and dynamically controlling the encoding [Fig. 4: 403] (page 11, lines 1-6) of the output data into an encoded output data [Fig. 4: 427] (page 12, lines 8-10) and the corresponding decoding [Fig. 4: 405] (page 11, lines 1-6) of the encoded output data [Fig. 4: 427] (page 12, lines 8-10) retrieved from the storage element [Fig. 4: 401] (page 12, lines 8-10).”

Independent claim 16 recites: “A method of processing cryptographic data, comprising: generating a mode signal having one of a given plurality of states; receiving a given input data and generating a cryptographic processed data output, said

generating including: generating a first input data, wherein the first input data is a selected one of a mask of the given input data and a not mask of the given data, the selection based on the state of the mode signal; generating a second input data, wherein the second input data is the other of the mask of the given input data and the not mask of the given data, performing a first set of logical operations [Fig. 3: 319] (page 10, lines 2-4) on the first input data to generate a first output data, the first set of logical operations [Fig. 3: 319] (page 10, lines 2-4) embodying a given input-output function, performing a second set of logical operations [Fig. 3: 321] (page 10, lines 2-4) on the second input data to generate a second output data, the second set of logical operations [Fig. 3: 321] (page 10, lines 2-4) being different (page 10, lines 14-18) than the first set of logical operations [Fig. 3: 319] (page 10, lines 2-4) and the second set of logical operations [Fig. 3: 321] (page 10, lines 2-4) embodying the same given input-output function, and merging [Fig. 3: 317] (page 9, lines 32-34) the first output data and the second output data to generate the cryptographic data output [Fig. 3: 333] (page 10, lines 21-23); repeating said generating a mode signal to have a different one of the given plurality of states; and repeating said receiving a given input data and generating a cryptographic processed data output.”

Dependent claim 2 recites: “a third combinatorial logical circuit [Fig. 5: 511] (page 13, lines 11-13), having an input, arranged to perform a third set of logical operations on an input data [Fig. 5: 569] (page 13, lines 22-23) at said input and to

produce a corresponding third output data [Fig. 5: 571] (page 13, lines 22-23), the third output data [Fig. 5: 571] (page 13, lines 22-23) having a third given functional relation to said input data [Fig. 5: 569] (page 13, lines 22-23) for input data [Fig. 5: 569] (page 13, lines 22-23) within a given range, and a fourth combinatorial logical circuit [Fig. 5: 513] (page 13, lines 11-13), having an input, arranged to perform a fourth set of logical operations on an input data [Fig. 5: 569] (page 13, lines 22-23) at said input and to produce a corresponding fourth output data, the fourth output data having a fourth functional relation to said input data [Fig. 5: 569] (page 13, lines 22-23) identical to said given third functional relation, wherein the third set of logical operations is different (page 13, lines 23-26) from the fourth set of logical operations, and a selector [Fig. 5: 563] (page 13, lines 31-33) for receiving said selected first cryptographic processing output data and dynamically selecting from among the third combinatorial logical circuit [Fig. 5: 511] (page 13, lines 11-13) and the fourth combinatorial logical circuit [Fig. 5: 513] (page 13, lines 11-13) for performing logical operations on the selected first cryptographic processing output data and producing a second output cryptographic processing data, and wherein said selecting includes inputting the selected first cryptographic processing output data to the input of the selected one of the third [Fig. 5: 511] (page 13, lines 11-13) and fourth [Fig. 5: 513] (page 13, lines 11-13) combinatorial logical circuits.”

Dependent claim 3 recites: “a selection circuit [Fig. 5: 563] (page 13, lines 33-34)

for generating a selecting signal to select one combinatorial logical circuit from among the first [Fig. 5: 507] (page 13, lines 11-13) and second [Fig. 5: 509] (page 13, lines 11-13) combinatorial logical circuits, a splitter circuit [Fig. 5: 543] (page 13, lines 14-15) for inputting the given input data [Fig. 5: 569] (page 13, lines 22-23) to one of the first [Fig. 5: 507] (page 13, lines 11-13) and second [Fig. 5: 509] (page 13, lines 11-13) combinatorial logical circuits, depending on the selecting signal, a merger circuit [Fig. 5: 553] (page 13, lines 31-33) for outputting data from one of the first [Fig. 5: 507] (page 13, lines 11-13) and second [Fig. 5: 509] (page 13, lines 11-13) combinatorial logical circuits, depending on the selecting signal.”

Dependent claim 4 recites: “a timing circuit [Fig. 4: 423] (page 10, lines 10-15) to determine the points in time at which the selection circuit [Fig. 4: 421] (page 10, lines 32-34) generates the selecting signal to select one of the first [Fig. 4: 403] (page 10, lines 10-15) and second [Fig. 4: 407] (page 10, lines 10-15) combinatorial logical circuits.”

Dependent claim 6 recites: “a second encoding means [Fig. 4: 407] (page 10, lines 10-15) for encoding the output data into a second encoded output data for storing in the storage element [Fig. 4: 401] (page 10, lines 10-15), a corresponding second decoding means [Fig. 4: 409] (page 10, lines 10-15), arranged for decoding the second encoded output data into said output data after retrieving the second encoded output data from the storage element [Fig. 4: 401] (page 10, lines 10-15), wherein the encoding of the

first output data is different from the encoding of the second output data, and wherein the electronic circuit is further arranged to generate a selecting signal to dynamically select from among the first encoding means [Fig. 4: 403] (page 10, lines 10-15) and its corresponding first decoding means [Fig. 4: 405] (page 10, lines 10-15) and the second encoding means [Fig. 4: 407] (page 10, lines 10-15) and its corresponding second decoding means [Fig. 4: 409] (page 10, lines 10-15), for encoding and decoding of the output data.”

Dependent claim 7 recites: “a timing circuit [Fig. 4: 423] (page 10, lines 10-15) to determine the points in time at which the electronic circuit selects one from among the first [Fig. 4: 403] (page 10, lines 10-15) and second [Fig. 4: 407] (page 10, lines 10-15) encoding means and corresponding first [Fig. 4: 405] (page 10, lines 10-15) and second [Fig. 4: 409] (page 10, lines 10-15) decoding means.”

Dependent claim 12 recites: “a first mask circuit [Fig. 1: 113] (page 7, line 5) for selectively masking and not masking, based on the signal, the given input data [Fig. 1: 129] (page 7, lines 8-9) for input to the first combinatorial logical circuit [Fig. 1: 101] (page 7, lines 1-3), and a second mask circuit [Fig. 1: 115] (page 7, line 5) for selectively masking and not masking, based on the signal, the given input data [Fig. 1: 129] (page 7, lines 8-9) for input to the second combinatorial logical circuit [Fig. 1: 103] (page 7, lines 1-3).”

Dependent claim 13 recites: “a first mask circuit [Fig. 1: 113] (page 7, line 5) to

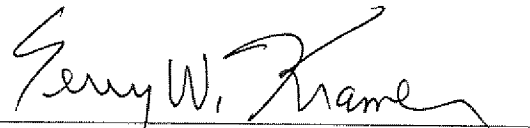
selectively mask and not mask, based on the signal, the given input data [Fig. 1: 129] (page 7, lines 8-9) and to input the selected masked and not masked given input data to the first combinatorial logical circuit [Fig. 1: 101] (page 7, lines 1-3), and a second mask circuit [Fig. 1: 115] (page 7, line 5) to selectively mask and not mask, based on the signal, to input the selected masked and not masked given input data [Fig. 1: 129] (page 7, lines 8-9) to the second combinatorial logical circuit [Fig. 1: 103] (page 7, lines 1-3).”

Dependent claim 15 recites: “wherein the selector [Fig. 1: 111] (page 7, lines 1-3) includes an OR merger circuit [Fig. 1: 109] (page 7, lines 1-3) to receive the output of the first combinatorial logical circuit [Fig. 1: 101] (page 7, lines 1-3) and to receive the output of the second combinatorial logic circuit [Fig. 1: 103] (page 7, lines 1-3), and to output, as the selected output [Fig. 1: 131] (page 7, lines 8-9), a logical OR of the output of the first combinatorial logical circuit [Fig. 1: 101] (page 7, lines 1-3) and the output of the second combinatorial logic circuit [Fig. 1: 103] (page 7, lines 1-3).”

CONCLUSION

In the event that the fees submitted prove to be insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account. Should there be any remaining issues that could be readily addressed over the telephone; the Examiner is asked to contact the attorney overseeing the application file, Juergen Krause-Polstorff, of NXP Corporation at (408) 474-9062.

Respectfully submitted,
KRAMER & AMADO, P.C.



Terry W. Kramer
Reg. No. 41,541

Date: September 8, 2010

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131
CUSTOMER NO.: 65913